IN THE SPECIFICATION

Please replace paragraph [0025] with the following amended paragraph:

[0025] Prior art systems typically allow a security administrator to set levels of security or authentication globally or establish the levels for a pre-selected group. FIG. 1 illustrates an exemplary embodiment of the present invention which allows a user to select a minimum security level for authentication for its own login to a restricted service. While using the functionality of this exemplary embodiment of the present invention to access a restricted service (e.g., an on-line service, a website, a webpage, a function, an individual application within a website, and/or the like) or a restricted area, a user is queried regarding the desired level of security for authentication (e.g., the user is queried to select one or more levels of security for authentication via a dialog box) (step 101). The user is typically a consumer desiring to access an on-line service, access a restricted area, purchase and/or sell a product, service or other item of commerce, otherwise transact in commerce, and/or communicate with another entity. The user may alternatively be a merchant, a distributor, a supplier, a person, an entity, software, hardware and/or the like desiring to transact or otherwise communicate with a consumer, a merchant, a distributor, a supplier, a person, an entity, software, hardware and/or the like. The user may interact with the system via any input device such as a computing unit, keyboard, mouse, smart card reader, biometric system, kiosk, personal digital assistant, handheld computer ~~(e.g., Palm Pilot®)~~ (e.g., Palm® Pilot), cellular phone and/or the like.

Please replace paragraph [0026] with the following amended paragraph:

[0026] The system facilitates a user's selection of a method of authentication for access to the restricted service, wherein the restricted service may require a method of authentication in order to gain access to the restricted service (e.g., the system allows the user to submit a level of security for authentication by entry of the selection into the dialog box) (steps 103-105). Alternatively, a host may select the minimum security level for authentication for the particular user based at least partially upon predetermined characteristics. In this exemplary embodiment of the present invention, the user may select between using a standard user identification and password entry into a user dialog box (step 103) or using a smart card and PIN authentication method (step 105) as the minimum level of security for authentication For example, a standard user identification and password can be created by the system or chosen by the user. In the same way, a PIN used with a smart card may be generated by the system or chosen by the user. Of course, any method of authentication may be used depending on the needs of the user and the functionality of the system providing the security level. Examples of other authentication methods include user identification and pass-phrase, biometric with or without a password (e.g., keyboard latency, fingerprint, palm print, eye/retina scan, voice recognition, and/or the like), smart card and digital certificate, ~~palm pilot~~ Palm® Pilot and digital certificate, sound verification, radio frequency and password, infrared and password, and/or the like.

Please replace paragraph [0031] with the following amended paragraph:

[0031] FIG. 2 illustrates an exemplary embodiment of the present invention, where the host may determine the minimum security level for authentication for the user based on

predetermined characteristics. A host may be one or more of the following: a server, a personal computer, a mainframe, a distributed network (e.g., the internet), a web service, and/or the like. There are many methods that the host may use in order to determine the user's selected security level for authentication. For example, the host may check for a cookie residing on the user's computing unit, wherein the cookie includes a desired level of authentication (step 201). The cookie resides on the user's computing unit by the user's prior access to the host, registration into the host system, or any other communication between the user and the host. The host may use any other method of identifying the user's selected security level for authentication via any identification method (e.g., profile stored on the host computer, user's personal computer, smart card, digital wallet, ~~palm pilot~~ Palm® Pilot, and/or the like). The host reads the preference set in the cookie, wherein the cookie includes information regarding the minimum level of security for authentication for the user (step 203). In this way, if the preference set includes information regarding the user's minimum level of security for authentication, the host may request the appropriate authentication information from the user. For example, if the cookie indicates that the user has selected to use the user identification and password authentication method (step 205), then a dialog box requesting a user identification and password is presented to the user via a web page (step 207). If the cookie indicates that the user has selected to use the smart card and PIN authentication method (step 209), then a dialog box requesting a smart card and PIN is presented to the user via a web page (step 211). On the other hand, if the preference set does not include information regarding the user's minimum level of security for authentication (e.g., the user is unknown) (step 213) or the user does not normally use the authentication methods provided by the host (steps 215 and 217), then a dialog box is

presented giving the user the option to register with the host and select an authentication method (step 219). For example, the user may be unknown if the user is a new user, the computing unit is new to the host, the user is accessing the host from a computing unit different from its usual point of access, and/or the like. After selecting a minimum level of security for authentication, the user may attempt to access a restricted service using the user selected method of authentication.